Data Processing Policy

Adopted by the HÖOK Hallgatói Szolgáltató Közhasznú Nonprofit Korlátolt Felelősségű Társaság (registered seat: H-1053 Budapest, Ferenciek tere 7-8., 1. em. 8., company registration number: 01-09-921744, tax number: 18087073-2-41, phone: +36/1/798-8134) (hereinafter: "Controller") 2018.

1/ General provisions

The subject of this data processing policy is the processing of personal data to be obtained by Controller in the context of organising the Skiride skiing camp (hereinafter: "Skiing Camp") on the basis of Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: "Information Act"), Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and other applicable laws.

This Policy shall lay down the data protection and data processing principles applied by Controller, through which Controller shall prevent the infringement of the personality rights of the individuals who shall be contacted during the services to be provided in the context of the Skiing Camp.

Controller shall reserve the right to unilaterally amend its data protection policy, including the content of this Policy, in case of modifying the services to be provided and in line with the applicable provisions of the law as amended from time to time. Controller shall immediately notify the data subjects on any change to this policy on the www.skiride.hu website.

2/ Data subjects affected by the data processing:

The natural persons (hereinafter: "data subjects") who enrol to and participate in the Skiing Camp.

3/ Purpose of the data processing:

Controller shall record and process the data subjects' voluntarily provided personal data for the following purposes related to the Skiing Camp provided by Controller and to the connected services: verification of the eligibility to participate in the Skiing Camp; keeping contacts as necessary in connection with the Skiing Camp; sending newsletter, providing information for advertising purposes.

4/ Legal basis of the processing and data source:

The primary legal basis of processing is the prior informed consent on the data processing provided by the data subjects, as well as the performance of the contract on the Skiing Camp as a service towards the data subjects.

The data source is the data provided voluntarily by the data subjects.

By providing his or her personal data in the contract, and with his or her declaration made in the knowledge of this policy, the data subject shall provide an explicit consent to the Controller processing his or her voluntarily provided personal data in accordance with the provisions of this policy.
If the data subject provides his or her data in the contract, such data shall be processed for the purposes specified in point 3, including the transfer of data. The data subject acknowledges that by accepting this policy he or she shall be considered to provide a *single consent to the processing of data for multiple purposes as specified above*.

The data subject may withdraw in writing, in an electronic mail his or her consent to the processing at any time without providing reasoning.

5/ Data pertaining to the data subjects, duration of processing:

Processing shall cover the following data of the data subjects:

- Name
- Personal ID card number
- Telephone number
- Email address

Providing the Controller with the above data shall be the precondition for concluding the contract and performing other services undertaken towards the data subject (sending newsletter, providing information for advertising purposes). In the absence of providing the data, the data subject shall not be able to conclude the contract and to use other services.

Processing shall commence upon filling out the contract and it shall cease by the expiry of two years from the date of filling. Upon the expiry of the duration of processing, Controller shall finally and irrecoverably delete the personal data of the data subjects.

6/ Type of transferred data:

Controller shall not use the personal data for any purpose other than specified herein, and it shall not transfer personal data to third persons without the data subject's prior informed consent, with the exception of any mandatory data transfer based on an Act.

7/ Obligations of Controller's employees during processing:

The personal data obtained by Controller shall only be accessed by Controller's employee contributing to the performance of the processing purposes specified in this policy, who shall be bound by an obligation of confidentiality on the basis of their labour contract, the provisions of the law applicable to their employment or Controller's instruction, concerning all data they have accessed.

Compliance with the data processing policy shall be mandatory for the Controller, all of its employees—including former employees—(hereinafter: "employee") during processing the data subjects' personal data.

Neither during the existence of the labour relationship, nor after its termination shall the employee be empowered to disclose, communicate to or make accessible by another person any personal data of the data subjects accessed during the labour relationship.
Employee may disclose to another employee the personal data accessed during the labour relationship if it is necessary for performing the work. Employee may only disclose to other third person the personal data accessed during the labour relationship with the approval of the person exercising the employer's rights. Employee may only take or transfer from the employer's registered office the personal data accessed during the labour relationship with the approval of the person exercising the employer's rights, irrespectively to the tool of taking or the method of transfer.

Employee shall notify without delay the person exercising the employer's rights if he or she becomes aware of the breach of this policy.
The general manager shall be responsible for Controller's activity, the compliance with this data processing policy.

8/ Technical management of the processing:

The method of recording the processed data may be as follows:

- printed document
- electronic data

The Controller shall implement appropriate technical and organisational measures to ensure the security of the personal data. Controller shall provide with appropriate protection (password, firewall) the IT equipment used for processing and storing personal data, and it shall guarantee that only authorised personnel shall have access to such equipment. Furthermore, Controller shall prevent the damaging, destroying or disclosure of the personal data also in the case of a force majeure.

9/ Rights of the data subjects related to processing

The data subject may request the Controller to:

• Provide information on the processing of his or her personal data: on the data subject's request, Controller shall provide, not later than within 30 days from receiving the request, information on the data subject's data processed by Controller, the sources of such data, the purpose, the legal basis and the duration of processing, as well as—in the case of transferring the data subject's personal data—the legal basis and the recipient of the data transfer. The provision of the information may only be refused in the cases regulated in an Act. Providing the information shall be free of charge, provided that in the current year the person requesting the information has not submitted to the Controller an information request concerning the same scope of data. In other cases the Controller may charge the expenses.

• Rectify his or her personal data: if the personal data is false and the correct personal data is available for the Controller, the controller shall rectify the personal data in its own competence, otherwise at the data subject request.

• Amend his or her personal data: if the personal data needs to be amended and the personal data to be amended is available for the Controller, the controller shall rectify the personal data in its own competence, otherwise at the data subject request.

• Delete his or her personal data: the Controller shall delete the personal data if its processing is unlawful; if it is requested by the data subject; if the purpose of processing no longer exists or the period for the storage of the data expires; if it is ordered by the court or an authority.

• Block his or her personal data: Controller shall block the personal data instead of deleting it, provided that it is requested by the data subject or it is presumed on the basis of the information available that the deletion would infringe the data subject's lawful interests. The personal data blocked in the above way may only be processed until the purpose of processing preventing the deletion of the personal data exists.

• Grant the transferability of his or her personal data: the right to receive from relevant Controller the personal data, which he or she has provided to Controller, in a commonly used and machine-readable format, and the right to transmit those data to another Controller.

In addition to the above, the data subject may also object to processing his or her personal data if the processing or the transfer of the personal data is necessary only for the purposes of fulfilling a legal obligation applicable to the Controller or the enforcement of the legitimate interests pursued by the controller, the recipient or by a third party.

The controller shall examine the objection as soon as possible upon submitting the application, but not later than within 15 days, and it shall decide about its reasonableness and inform the applicant about the decision in writing.
The above rights are detailed in Sections 14 to 19 and Section 21 of the Information Act. The data subject may turn to the court in the case of the violation of his or her rights and in other cases laid down in the Information Act (Section 23 of the Information Act). Judging upon the action shall fall in the competence of the regional court. The action may be also brought before the regional court having jurisdiction according to the data subject’s place of residence or place of stay—in his or her discretion.

Furthermore, the data subject may file a complaint to the National Authority for Data Protection and Freedom of Information regarding the processing he or she considers to be unlawful.

10/ Special rules on sending a newsletter and information for advertising purposes

Controller shall send to the data subjects a message containing information primarily related to the purpose of processing and other services provided by Controller in the context of using such services.

At the same time the data subject acknowledges that subscription to the newsletter service shall be considered as a consent within the meaning of Section 6(1) of Act XLVIII of 2008 on the Basic Conditions and Certain Limitations of Business Advertising, on the basis of which Controller may forward direct advertising and marketing requests to the electronic mailing address provided by the

data subject. By subscribing to the newsletter service, the data subject shall provide explicit consent to Controller sending him or her news, newsletters, advertisements and promotion offers related to the services provided by Controller.
Should the data subject wish not to receive in the future messages containing advertisements, he or she may unsubscribe by using the option offered in the newsletter sent by Controller, and he or she may explicitly prohibit personally or in a postal or electronic mail addressed to Controller the sending of requests containing advertisements.

11/ Closing provisions

The data subject hereby acknowledges and agrees that Controller may disclose on its own social media profile the recordings of images and sound made during the provision of services provided by Controller, even if the data subject is depicted there in an individually recognisable way. The data subject may request the removal of the disclosed recording if his or her personality rights are infringed.

Controller shall provide compensation for the damages caused to others by the unlawful processing of the data subject's data or by breaching the requirements of data security, unless the damage is the result of the wilful or gravely negligent conduct of the person suffering the damage.

Matters not regulated in this policy shall be governed by the provisions of Act V of 2013 on the Civil Code, Act CXII of 2011 on Informational Self-Determination and Freedom of Information, Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and other applicable laws.

This General Terms and Conditions shall be valid from the day until revocation.